CHAPTER 14

INFORMATION TECHNOLOGY CONTROLS

SCOPE

This chapter addresses requirements common to all financial accounting systems and is not limited to the statewide financial accounting system, ENCOMPASS, but also applies to subsystems used by the various agencies of the State of Indiana to create and store financial information.

In the event these requirements are not met by the computer environment of the accounting system, compensating manual controls must be implemented.

Table of Contents

14.1 AUDITING STANDARDS 2

14.2 INTERNAL CONTROLS 2

14.3 BUSINESS PROCESSES 2

14.3.1 Disaster Recovery 2

14.3.2 Backup Processing 2

14.3.3 Physical Security 3

14.3.4 Logical Security 3

14.3.5 Audit Trails 4

14.3.6 Input Controls 4

14.3.7 Output Controls 4

14.3.8 Interface Controls 5

14.3.9 Internal Processing 5

14.3.10 Error Correction 5

14.3.11 Change Controls 6

14.3.12 Programming Documentation 6

14.3.13 Operations Documentation 6

14.3.14 User Documentation 7

14.3.15 Information Retention and Access 7

14.1 AUDITING STANDARDS

In accordance with Statements on Auditing Standards Numbers 78 and 94, issued by the American Institute of Certified Public Accountants (AICPA), the State Board of Accounts may review any computer system that processes accounting data. Selection of the computer systems to be reviewed and the scope of the reviews will be based on the following criteria: total dollars processed by the computer system, the materiality of those dollars to the unit's financial statements, the complexity of the processing, the availability of alternate sources for audit information, and the criticality of non-financial information processed. The Information Technology (IT) controls reviewed will be based primarily on the Control Objectives for Information and Related Technology (COBIT) and other publications of the Information Systems Audit and Control Association. Additional sources of information used in State Board of Accounts' IT reviews include but are not limited to publications of the AICPA, the Institute of Internal Auditors, the Government Accountability Office, the Department of Defense, the National Computer Security Association, and hardware and software vendors.

14.2 INTERNAL CONTROLS

Governmental units should have internal controls in effect which provide reasonable assurance regarding the reliability of financial information and records, effectiveness and efficiency of operations, proper execution of managements' objectives, and compliance with laws and regulations. Segregation of duties and safeguarding controls over cash, all other assets, and all forms of information processing are necessary for proper internal control.

Segregation of duties is the concept of having different people do different tasks within the organization. It provides the foundation of good internal control by assuring that no one individual has the capability to perpetuate and conceal errors or irregularities in the normal course of their authorized duties. Segregation of duties is achieved within information technology systems by appropriate assignment of security profiles that define the data the users can access and the functions that they can perform. Access must be restricted to the minimum required for the user to perform their job function. Access rights must be periodically reviewed and approved by management.

14.3 BUSINESS PROCESSES

14.3.1 Disaster Recovery

A written Disaster Recovery Plan is required to ensure that critical accounting information will be processed in the event of interruption of computer processing capability. The plan must be updated and tested annually or when significant modifications to computer hardware, software or application systems occur. One copy of the Plan must be retained offsite.

14.3.2 Backup Processing

All computer application programs and operating system software must be backed up on a periodic basis and after modification. Accounting information must be backed up on a periodic basis

sufficient to allow restoration of the information in a timely manner. Periodically the backup media must be tested to ensure restoration will occur accurately. One copy of the backup information must be retained offsite.

14.3.3 Physical Security

The computer system and the associated telecommunications equipment must be adequately protected from environmental damage including, but not limited to, fire, water, and physical damage by individuals. In addition, the computer must be protected from unauthorized access, terminals must be inoperable when not attended by an authorized employee, and terminals utilized to enter sensitive commands must not be positioned where unauthorized individuals may view the contents of the video display terminal.

14.3.4 Logical Security

Effective logical security prohibits unauthorized access and restricts the computerized resources each authorized user may utilize. Access to accounting information and processes must be controlled by operating system software and by the computerized accounting application through user identification codes (user IDs) and passwords. User IDs are unique identifiers assigned to each authorized user, which remain constant for that user. Passwords are confidential keywords associated with the user ID to provide verification of the user's identity. Each user must have a unique user ID and password which must not be shared. Passwords must meet the following criteria:

- *Passwords must be changed frequently to prevent misuse.*
- *Passwords must be a minimum of six (6) characters in length.*
- *Passwords must be a combination of alphabetic and numeric characters.*
- *Passwords may not be the same for a user ID as the last five (5) passwords used by this user ID.*
- *Individuals must assign their own passwords.*
- *Passwords must be encrypted while stored on the computer.*

Additional Logical Security requirements include:

- *Reporting of user access rights to system functional capabilities and information, as well as reporting of security definitions such as configuration parameters, workflow approval hierarchy, thresholds, and override capabilities must be available to, and easily understood by, management and State Board of Accounts' Field Examiners during the course of a regularly scheduled audit. These security definitions and user access rights must enforce adequate segregation of duties for the accounting system.*
- *Users other than System Administrators and Security Administrators must be prevented from accessing sensitive operating system commands.*
- *The number of System Administrators and Security Administrators must be limited.*
- *Computer programmers must not have update access to production accounting information.*
- *Users must not be allowed to be active on multiple terminals at the same time with the same user ID.*

- *User IDs must be deactivated after three unsuccessful attempts to sign on to the computer.*
- *For inactive terminals, the user must be automatically prevented from accessing the computer after 15 minutes of no activity until the user's password is entered.*
- *Users must be prevented from modifying or deleting operating system and computer program files.*
- *Users must be prevented from updating accounting information except through authorized transactions and processes within the computerized accounting application system.*
- *User access rights must be eliminated or revised upon termination of employment and transfers of employee responsibility.*

14.3.5 Audit Trails

The computerized accounting system must maintain electronic audit trails sufficient to trace all transactions from the original source of entry into the system, through all system processing, though various levels of summarizations, and to the results produced by the system. The audit trails must also maintain sufficient information to trace all transactions from the final results produced by the system, through all system processing and summarizations, and to the original source of entry into the system. Audit trails must also identify the user that processed the transaction or updated the information. These audit trails must be protected from modification and deletion.

14.3.6 Input Controls

The computerized accounting system must provide input edits and controls to ensure that information entered into the system is accurate, that all appropriate information is entered into the system, and that information is entered into the system only once. All information entered into the system must be authorized through effective manual or electronic controls.

Transaction dates should be based upon system generated dates which cannot be modified by the user. If necessary, the system may provide an additional effective date of the transaction that is user controlled. However, controls must exist to ensure effective dating does not result in data integrity, reporting, and reconcilement problems. In addition, accounting periods should be promptly closed to ensure transactions can only be posted to the current period.

14.3.7 Output Controls

The computerized accounting system must incorporate features that ensure all accounting information is reported accurately and completely. Procedures must also exist to ensure that only authorized individuals have access to computer generated output. All receipts or payments generated by the accounting system must include unique document identification numbers either preprinted on the form or printed on the form by the application system. If the numbers are printed on the form by the application system, adequate security must be implemented to prevent unauthorized modification of the number sequence. Preprinted receipt and check stock must not include preprinted signatures, must be securely stored, and usage must be logged and reconciled. If the report content can be modified via user selection of various criteria such as account codes, department codes, transaction codes, status codes, dates, etc., the report heading should contain sufficient information regarding the selection criteria to allow another user to understand what information is being reported and recreate the report. All output reports must clearly indicate the effective dates of the information in addition to the report generation date. Output reports must have appropriate subtotals to allow reconcilement to other reports and to external documentation.

14.3.8 Interface Controls

Information generated in one computer application system and transferred to another computer application system must be accurate and complete. Both systems should generate reports documenting record counts and the dollar value totals of the information transferred to enable prompt identification of discrepancies.

Intra–system transfers of information (between modules and subsystems of the same computer application) should also be controlled and reconciled. Ideally this should be accomplished automatically by system processes and include appropriate error and out-of-balance reports. Alternatively the system should produce sufficient information to allow manual verification of whether information was transferred completely and accurately, and to identify errors, reconcile subsidiary ledgers to control ledgers, and reconcile detail transactions to summary totals.

14.3.9 Internal Processing

Automated processes that support the unit's business processes should operate accurately, efficiently and completely. The system should accurately calculate, summarize, categorize and update accounting information. The system should allow for effective and efficient reconciliation of subsidiary ledgers to control ledgers, and detail transactions to summary totals. The system should automatically identify erroneous input, prevent concurrent file updates, and generate control totals to ensure completeness of processing. The system should also include standard controls such as tables which ensure only valid values can be posted, suspense files to identify transactions that fail system edits, effective error messages, appropriate restore points, and methods to prevent or detect out-of-balance conditions.

14.3.10 Error Correction

The accounting application should provide extensive data editing, validation, and change capability upon input and before a transaction is posted to an account, but no ability to change data after it is posted. If an error is discovered after the transaction is posted, a separate correcting transaction must be made.

Accounting information must not be modified by computer utility programs which are not contained in the accounting application system. The accounting application system must be supported by computerized and manual procedures to ensure the following error correction controls are implemented:

- *The type of error condition is recorded.*
- *The original transaction creating the error is retained within the system.*
- *A reversing transaction to eliminate the effect of the error is entered and retained within the system.*
- *The correct transaction is entered into the system and recorded.*
- *Management approval for error correction is documented.*

14.3.11 Change Controls

Changes to the accounting system's computer programs must be adequately controlled including the following requirements:

- *Computer source (human readable) and load (machine readable) modules must be protected from unauthorized modification.*
- *Modifications to computer source code must occur in a test environment and not affect production source code.*
- *All modifications to computer source code must be adequately tested. Modifications must be approved by management.*
- *Individuals responsible for modifying computer source code in a test environment must be prevented from updating computer code in the production environment. Movement of computer source and load modules from the test to production environments must be completed by authorized employees not responsible for modification of computer source or load modules.*

Various other system components such as configuration parameters and control tables can also have a significant impact on the way the system operates and processes information without changing actual program code. Changes to these system components should also be controlled by similar mechanisms.

14.3.12 Programming Documentation

During the course of a regularly scheduled audit, documentation must be available to the State Board of Accounts' Field Examiners that provides adequate information on the functions performed by each computer program, the definitions of all computer files and records utilized by the computer programs, and a description of the computer processing which relates each computer program to other computer programs to accomplish accounting functions. The documentation must be adequate for the Field Examiners to determine how the computer system processes accounting information.

14.3.13 Operations Documentation

For each computerized accounting system, procedures must be adequately documented to ensure all processing and maintenance is performed. Examples include instructions, checklists, and logs to ensure:

- *Daily, monthly and year-end processes are performed correctly and completely.*
- *Required reports are generated and balanced.*
- *Backups are completed successfully and cycled appropriately.*
- *Virus definitions are updated regularly.*
- *Security patches and upgrades are installed.*

14.3.14 User Documentation

Written procedures must be available for all computerized accounting systems which provide instructions on the requirements for the approval of information prior to entry into the computer, as well as the accurate entry, processing, and reporting of information from the accounting system.

14.3.15 Information Retention and Access

A detailed transaction history (similar to a manually posted ledger page) must be maintained supporting each account. At least the last twelve months of transactions must be accessible on-line. Additional transactional history must be retained back to the date of the last audit. This additional history must be retained on-line or otherwise archived and easily accessible by State Board of Accounts' Field Examiners. Records should also be retained in compliance with the appropriate retention schedule as approved by the Indiana Commission on Public Records.

Public records, financial statement information, and supporting information generated through the computer system must be maintained in a manner that will allow access for audit and public inquiry. Acceptable mechanisms include hardcopy, on equipment provided by the governmental unit, or via the Internet.